

IN THE CLAIMS

For the convenience of the Examiner, all pending claims of the present Application are presented below whether or not an amendment has been made. Please amend the claims as follows:

1. (Original) A method of selecting a detection method for analyzing computer code for malicious code, comprising:

providing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code;

selecting a fastest one of the malicious code detection methods;

analyzing computer code for malicious code using the selected malicious code detection method;

determining a probability of accuracy of a result of the analysis;

selecting a next fastest one of the malicious code detection methods and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level; and

outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

2. (Original) A method of selecting a detection method as recited in claim 1, wherein at least some of the malicious code detecting methods use heuristic logic to detect for malicious code.

3. (Original) A method of selecting a detection method as recited in claim 1, wherein the fastest one of the malicious code detecting methods is a least accurate one of the plurality of malicious code detecting methods.

4. (Original) A method of selecting a detection method as recited in claim 1, wherein a slowest one of the malicious code detecting methods is a most accurate one of the plurality of malicious code detecting methods.

5. (Original) A method of selecting a detection method as recited in claim 1, further comprising prompting a user to input a value to be used as the predetermined level.

6. (Original) A method of selecting a detection method as recited in claim 5, further comprising receiving the value input by the user and using the value as the predetermined level.

7. (Original) A system for selecting a detection method for analyzing computer code for malicious code, comprising:

means for storing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code;

means for selecting a fastest one of the malicious code detection methods;

means for analyzing computer code for malicious code using the selected malicious code detection method and outputting a result of the analysis;

means for determining a probability of accuracy of the result of the analysis;

means for selecting a next fastest one of the malicious code detection methods and repeating the analyzing and determining, if the probability of accuracy is below a predetermined level; and

outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

8. (Original) A system for selecting a detection method as recited in claim 7, wherein at least some of the malicious code detecting methods use heuristic logic to detect for malicious code.

9. (Original) A system for selecting a detection method as recited in claim 7, wherein the fastest one of the malicious code detecting methods is a least accurate one of the plurality of malicious code detecting methods.

10. (Original) A system for selecting a detection method as recited in claim 7, wherein a slowest one of the malicious code detecting methods is a most accurate one of the plurality of malicious code detecting methods.

11. (Original) A system for selecting a detection method as recited in claim 7, further comprising means for prompting a user to input a value to be used as the predetermined level.

12. (Original) A system for selecting a detection method as recited in claim 11, further comprising means for receiving the value input by the user and using the value as the predetermined level.

13. (Original) A storage medium including computer executable code for selecting a detection method for analyzing computer code for malicious code, the computer executable code comprising:

code including a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code;

code for selecting a fastest one of the malicious code detection methods;

code for analyzing computer code for malicious code using the selected malicious code detection method;

code for determining a probability of accuracy of a result of the analysis;

code for selecting a next fastest one of the malicious code detection methods and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level; and

code for outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

14. (Original) A storage medium as recited in claim 13, wherein at least some of the malicious code detecting methods use heuristic logic to detect for malicious code.

15. (Original) A storage medium as recited in claim 13, wherein the fastest one of the malicious code detecting methods is a least accurate one of the plurality of malicious code detecting methods.

16. (Original) A storage medium as recited in claim 13, wherein a slowest one of the malicious code detecting methods is a most accurate one of the plurality of malicious code detecting methods.

17. (Original) A storage medium as recited in claim 13, further comprising code for prompting a user to input a value to be used as the predetermined level.

18. (Original) A storage medium as recited in claim 17, further comprising code for receiving the value input by the user and using the value as the predetermined level.

19. (Original) A programmed computer system including computer executable code for selecting a detection method for analyzing computer code for malicious code, the system comprising:

storage for storing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code;

a unit for reading and executing computer executable code, the computer executable code comprising,

code for selecting a fastest one of the malicious code detection methods,

code for analyzing computer code for malicious code using the selected malicious code detection method,

code for determining a probability of accuracy of a result of the analysis, and

code for selecting a next fastest one of the malicious code detection methods and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level; and

an output unit for outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

20. (Original) A programmed computer system as recited in claim 19, wherein at least some of the malicious code detecting methods use heuristic logic to detect for malicious code.

21. (Original) A programmed computer system as recited in claim 19, wherein the fastest one of the malicious code detecting methods is a least accurate one of the plurality of malicious code detecting methods.

22. (Original) A programmed computer system as recited in claim 19, wherein a slowest one of the malicious code detecting methods is a most accurate one of the plurality of malicious code detecting methods.

23. (Original) A programmed computer system as recited in claim 19, further comprising a unit for prompting a user to input a value to be used as the predetermined level.

24. (Original) A programmed computer system as recited in claim 23, further comprising a unit for receiving the value input by the user and using the value as the predetermined level.

25. (Original) A method of selecting a detection method for analyzing computer code for malicious code, comprising:

providing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods have different expected degrees of accuracy when analyzing for malicious code;

selecting a malicious code detection method having a lowest expected degree of accuracy;

analyzing computer code for malicious code using the selected malicious code detection method;

determining an actual probability of accuracy of a result of the analysis;

selecting a next least accurate malicious code detection method and repeating the analyzing and determining steps, if the actual probability of accuracy is below a predetermined level; and

outputting a result of the analysis if the actual probability of accuracy is at or above the predetermined level.

26. (Original) A system for selecting a detection method for analyzing computer code for malicious code, comprising:

means for storing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods have different expected degrees of accuracy when analyzing for malicious code;

means for selecting a malicious code detection method having a lowest expected degree of accuracy;

means for analyzing computer code for malicious code using the selected malicious code detection method and outputting a result of the analysis;

means for determining an actual probability of accuracy of the result of the analysis;

means for selecting a next expected least accurate malicious code detection method and repeating the analyzing and determining, if the actual probability of accuracy is below a predetermined level; and

outputting a result of the analysis if the actual probability of accuracy is at or above the predetermined level.

27. (Original) A storage medium including computer executable code for selecting a detection method for analyzing computer code for malicious code, the computer executable code comprising:

- code including a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods have different expected degrees of accuracy when analyzing for malicious code;

- code for selecting a fastest one of the malicious code detection methods;

- code for analyzing computer code for malicious code using the selected malicious code detection method;

- code for determining an actual probability of accuracy of a result of the analysis;

- code for selecting a next expected least accurate malicious code detection method and repeating the analyzing and determining steps, if the actual probability *of* accuracy is below a predetermined level; and

- code for outputting a result of the analysis if the actual probability of accuracy is at or above the predetermined level.

28. (Original) A programmed computer system including computer executable code for selecting a detection method for analyzing computer code for malicious code, the system comprising:

- storage for storing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods have different expected degrees of accuracy when analyzing for malicious code;

- a unit for reading and executing computer executable code, the computer executable code comprising,

- code for selecting a malicious code detection method having a lowest expected degree of accuracy,

- code for analyzing computer code for malicious code using the selected malicious code detection method,

- code for determining an actual probability of accuracy of a result of the analysis,
- and

- code for selecting a next expected least accurate malicious code detection method and repeating the analyzing and determining steps, if the actual probability of accuracy is below a predetermined level; and

- an output unit for outputting a result of the analysis if the actual probability of accuracy is at or above the predetermined level.

29. (Original) A method of selecting a detection method for analyzing computer code for malicious code, comprising:

- providing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require use of different amounts of computer resources to analyze for malicious code;

- selecting a malicious code detection method requiring use of the least amount of computer resources;

- analyzing computer code for malicious code using the selected malicious code detection method;

- determining a probability of accuracy of a result of the analysis;

- selecting a malicious code detection method requiring the use of the next least amount of computer resources and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level; and

- outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

30. (Original) A system for selecting a detection method for analyzing computer code for malicious code, comprising:

means for storing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require use of different amounts of computer resources to analyze for malicious code;

means for selecting a malicious code detection method requiring the use of the least amount of computer resources;

means for analyzing computer code for malicious code using the selected malicious code detection method and outputting a result of the analysis;

means for determining a probability of accuracy of the result of the analysis;

means for selecting a malicious code detection method requiring the next least amount of computer resources and repeating the analyzing and determining, if the probability of accuracy is below a predetermined level; and

outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

31. (Original) A storage medium including computer executable code for selecting a detection method for analyzing computer code for malicious code, the computer executable code comprising:

code including a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require use of different amounts of computer resources to analyze for malicious code;

code for selecting a malicious code detection method requiring the use of a least amount of computer resources;

code for analyzing computer code for malicious code using the selected malicious code detection method;

code for determining a probability of accuracy of a result of the analysis;

code for selecting a malicious code detection method requiring use of the next least amount of computer resources and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level; and

code for outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.

32. (Original) A programmed computer system including computer executable code for selecting a detection method for analyzing computer code for malicious code, the system comprising:

- storage for storing a plurality of malicious code detection methods, wherein at least some of the malicious code detection methods require use of different amounts of computer resources to analyze for malicious code;

- a unit for reading and executing computer executable code, the computer executable code comprising,

- code for selecting a malicious code detection method requiring use of a lowest amount of computer resources,

- code for analyzing computer code for malicious code using the selected malicious code detection method,

- code for determining a probability of accuracy of a result of the analysis, and

- code for selecting a malicious code detection method requiring use of a next least amount of computer resources and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level; and

- an output unit for outputting a result of the analysis if the probability of accuracy is at or above the predetermined level.